信任评估方案

# 基于零信任的远程桌面系统架构



基于零信任的远程桌面系统主要由接入终端、接入网关、云服务器及其上部署的虚拟机、接入控制器、统一身份认证系统、零信任网关和业务系统等主要部件构成。在使用时，接入终端首先需要建立与接入控制器之间的零信任连接，然后访问接入控制器，通过接入控制器选择云服务器中的虚拟机。此时，接入终端会向接入控制器请求访问权限，待得到接入控制器的零信任认证，获取信任凭证后，即可访问虚拟机。在访问虚拟机时，流量首先通过接入网关进行转发，再由云服务器中的人机交互协议模块解码，随后传送到虚拟机。用户登录虚拟机后，使用虚拟机通过零信任网关访问业务系统，这一过程首先需要虚拟机通过信任传递机制获取到终端在前述认证过程中得到的信任凭证，然后利用该凭证以类似的过程取得接入控制器的零信任认证，认证通过后方可访问业务系统。上述访问控制过程全程采用了零信任技术，接入控制器中设计了零信任控制组件，其中包括了实时信任评估和策略管理两项功能，访问控制由策略管理相关功能下发策略信息到网关实现。因此，不仅在首次认证时可以控制用户的访问，在用户使用虚拟机访问业务系统的全过程中，均可实现零信任访问控制。

# 总体思路

本方案面向零信任架构下的远程桌面系统信任评估和动态访问控制的需求，设计了一个融合多维特征、图结构传播与动态决策机制的联合信任评估模型。模型分别从用户节点、接入终端节点和虚拟机节点三类实体出发，采集其身份属性、行为模式与风险状态，通过归一化与压缩映射等方法处理特征数据，并以加权形式计算局部信任评分。基于用户与终端、终端与虚拟机之间的访问链路，进一步构建信任传播图，将虚拟机行为信息传递至终端，终端信任度再反馈至用户，实现行为链闭环下的信任增强推理。最终的信任评分被用于实时动态访问控制策略生成，包括二次认证、访问限制与阻断等策略，实现访问路径中的全链路控制能力。

# 特征采集

本发明设计了一种联合信任得分计算模型。该模型综合考虑终端侧的身份强度、行为稳定性、安全状态等因素，以及虚拟机侧的运行状态、安全属性与资源占用情况，通过多维指标聚合函数分别计算其局部信任得分。同时，引入动态权重机制，使终端与虚拟机的得分权重随时间或行为变化自适应调整，增强时效性和风险敏感性。模型还创新性地引入非线性耦合函数，衡量终端行为与虚拟机使用行为之间的一致性程度，从而实现行为链闭环下的信任增强推理。最终得分还结合信任衰减项，防止长期静态授权带来的安全隐患。该联合信任模型支持细粒度动态访问控制策略的实时生成与调整，能够有效提升远程桌面环境下的安全防护能力与访问精确性。

## 云接入管理平台提供的基础接口

### 系统日志接口

系统日志接口中可以查询到终端用户登录次数：

#### （1）URL

GET /api/v1/log/syslog/list

#### （2）请求体

[{"name":"bizCode","type":"Eq","value":"client.bizApi.userAuth"},{"name":"logTime","type":"TimeRange","value":"[\"2025-05-09 00:00\",\"2025-06-07 23:59\"]"},{"name":"logSubject","type":"Eq","value":"test01"}]

#### （3）响应体

Response body:

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"logId": "xxx",

"fromSource": "client",

"module": "client.bizApi",

"bizCode": "client.bizApi.userAuth",

"logLevel": "info",

"logTime": "2025-06-06 12:48:14.000",

"logProducer": "system",

"logSubject": "test01",（账号）

"logLocation": "172.16.40.146",

"logObject": "test",（设备ID）

"logResult": "success",

"content": "test01 通过终端类型：软终端 ip地址：172.16.40.146 设备编号：test的终端执行了 用户认证，结果：成功"

}

],

"totalCount": 1

}

### 终端用户查询接口

#### （1）URL

GET /api/v1/user/local/list

#### （2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"userId": "ff80808196b4c4050196d6e96f060087",

"userName": "test",

"userType": "AdUser",

"account": "test01",

"domain": "xxx",

"createTime": "2006-01-02 15:04:05.999",

"createUser": "cloudadmin",

"email": "123@qq.com",

"phone": "13858585858",

"state": "Enable",

"syncType": "A",

"updateTime": "2006-01-02 15:04:05.999",

"updateUser": "cloudadmin",

"userLoginIpControl": [

{

"startIp": "172.16.5.1",

"endIp": "172.16.5.66"

}

]

}

],

"totalCount": 1

}

### 3.1.3 管理员用户查询接口

#### （1）URL

GET /api/v1/admin-user/list

#### （2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"userId": "ff80808196a34f1801974548e37a405a",

"userName": "system admin"

"account": "sysadm",

"email": "123@qq.com",

"mobileNumber": 13858585858,

"pwdErrorNum": 0,

"userLoginIpControl": [

{

"startIp": "172.16.0.1",

"endIp": "172.16.0.2"

}

],

"userState": 1,

"userType": "AdminUser",

"lockTime": "2025-06-16 11:07:21",

"createdTime": "2025-06-16 11:06:51",

"expirationTime": "2025-06-16 11:06:51"

}

]

"totalCount": 1

}

### 3.1.4接入终端查询接口

（1）URL

GET /api/v1/terminal/mgt/list

（2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"terminalId": "4152915abc2c34c9ae58c004402dbabf",

"endpointId": "8765915abc2c34c9ae58c006544xxxxx",

"accessIp": "172.16.40.33",

"archType": "aarch64",

"ip": "172.16.40.33",

"mac": "90:E2:FC:B6:0A:C6",

"osType": "vfirmware",

"osVersion": "1.0.0",

"regFirstTime": 1746524325000,

"regUpdateTime": 1746524325000,

"state": "Enable",

"terminalOs": "vFirmware-JT301-1.0.0",

"terminalType": "TC",

"terminalVersion": "2.0.7",

"workState": "Online",

"lastLoginUserId": "ff80808196a4f5b80196a5065b360014",

"lastLoginUserName": "vxum",

}

],

"totalCount": 1

}

### 3.1.5 Session在线会话查询接口

#### （1）URL

GET /api/v1/session/list

#### （2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"sessionId": "556aefc539704ba8a36756717b40e14a",

"sessionState": "Connected",

"connectStart": "2006-01-02 15:04:05.999",

"onlineTime": 82223,

"resourceGroupId": "ff808081966c2d6d01966c5710aa0061",

"resourceId": "ff80808196a34f1801973500bd6b39ae",

"resourceCode": "ubuntu\_104\_118",

"orgName": "RD",

"userName": "jstack\_test002",

"userId": "ff808081966c2d6d01966c55830f0045",

"userType": "LocalUser",

"account": "jstack\_test002",

"terminalIp": "172.16.40.105",

"agentIp": "192.168.104.118"

}

],

"totalCount": 1

}

### 3.1.6 历史会话查询接口

#### （1）URL

GET /api/v1/session/history/list

#### （2）响应体

Response body:

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"sessionId": "556aefc539704ba8a36756717b40e14a",

"sessionState": "Connected",

"connectStart": "2006-01-02 15:04:05.999",

"connectEnd": "2006-01-02 15:04:05.999",

"onlineTime": 82223,

"disconnectReason": "Disconnected",

"resourceGroupId": "ff808081966c2d6d01966c5710aa0061",

"resourceId": "ff80808196a34f1801973500bd6b39ae",

"resourceCode": "ubuntu\_104\_118",

"orgName": "RD",

"userName": "jstack\_test002",

"userId": "ff808081966c2d6d01966c55830f0045",

"userType": "LocalUser",

"account": "jstack\_test002",

"terminalIp": "172.16.40.105",

"agentIp": "192.168.104.118"

}

],

"totalCount": 1

}

### 3.1.6 虚拟机查询接口

#### （1）URL

/manager/api/manager/platform/listDeviceByPage

#### （2）响应体

{

"returnCode": "0",

"total": 16,

"data": [

{

"deviceStorage": "120",

"deviceIp": "192.168.102.235",

"resourceId": "ff808081966c287e01966c29133a0028",

"deviceRegMode": "1",

"deviceOs": "Linux-Kylin-v10",

"resourceName": "Kylin10\_x64\_102\_235",

"deviceCode": "0000000000000133",

"deviceMemory": "8",

"platformId": "ff808081966c2d6d01966c4f29fc0003",

"deviceId": "ff808081966c287e01966c291387002b",

"deviceName": "kylin-2403-chenrw02郭亮",

"deviceCpu": "{\"Type\":\"未知\",\"Num\":\"8\"}",

"hostCapabilityType": "SingleSession",

"createTime": "2025-01-24 10:46:25",

"deviceIpv6": "",

"hasIpmi": false,

"deviceMac": "52:54:00:80:93:6B",

"devicePort": 5061,

"resourceMgmtCode": "000001005",

"deviceState": "Running",

"platformName": "Jstack\_100\_31",

"platformCode": "WiserSoft",

"workingState": "Running"

}

],

"success": true

}

### 3.1.7 性能采集接口

#### （1）URL

GET /api/v1/resource-platform/vm/metrics

虚拟机处于运行种才能返回，resourceId 为必传参数，URL中过滤参数：[{"name":"resourceId","type":"In","value":["ff8080819753bbf701975df63e430027"]}]

#### （2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"resourceId": "xxx",

"cpuRate": "CPU利用率",

"memFree": "内存空闲，byte",

"memTotal": "内存总量，byte"

}

],

"totalCount": 1

}

### 3.1.8 资源列表接口

#### （1）URL

GET /api/v1/resource/list

#### （2）响应体

Response body：

{

"traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",

"resultCode": "Success",

"message": "Success",

"data": [

{

"resourceId": "ff80808196a4f5f80196a4f664080003",

"resourceCode": "525400F6ED0E",

"resourceName": "testRes",

"devicePlatformId": "ff80808196a515de0196a517b1bb0001",

"devicePlatformName": "cam\_test\_盛思睿",

"deviceCode": "0000000000000002",（虚拟机编码）

"deviceId": "ff80808196a4f5f80196a4f65fcc0000",

"deviceName": "win10-104",

"ip": "127.0.0.1",

"ipV6": "",

"agentPort": 5064,

"mac": "52:54:00:F6:ED:0E",

"os": "Windows-10",

"deviceState": "Running",

"resourceState": "Online",

"resourceRegFlag": "Registered",

"resourceAssignState": "Available",

"agentVersion": "2.0.7"

}

],

"totalCount": 1

}

## 3.2特征采集与向量构建

### （1）用户（User）节点：

采集特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **特征类型** | **特征名称** | **符号定义** | **数据类型** | **说明** |
|  | 其他 | 账号类型 | userType | 整型 | 在信任评估模块初始化阶段调用管理员查询接口获得管理员账户列表，如果一个账户在列表内就认为是管理员，否则就是普通用户。管理员账户列表由信任评估模块维护。  管理员：1  普通用户：0 |
|  | 信任值阈值 | thresholdDelta | 浮点型 | 根据历史信任评估行为得到的信任阈值，即低于该阈值就触发二次认证 |
|  | 登录频次 | 尝试登录次数 | loginTotal | 整型 | 查询日志数据库，获得一个用户一段时间内尝试登录的次数。 |
|  | 登录成功次数 | loginSucceed | 整型 | 查询日志数据库，获得一个用户一段时间内登录成功的次数。 |
|  | 登录时间 | 登录时间段是否存在异常 | ifLoginTimeOK | 整型 | 信任评估触发后，利用在线会话查询接口获得当前活跃的会话，记录每个活跃会话的connectStart，更新User数据库中的登录时间，并查询信任评估规则，判断本次登录的时间段是否符合规则约定，如上午/中午，如果没有相关规则，则视为在允许的时间段登录。  符合：1  不符合：-1 |
|  | 是否偏离习惯登录时间段 | LoginTimeBias | 浮点型 | 信任评估触发后，利用历史会话查询接口获取单位时间窗口内的登录记录，并存于数据库中的History表。根据过去十次登录时间段计算平均登录时间，本次登录时间-登录时间中位数/24 |
|  | 最近访问时间距离当前时刻的时间差 | LoginTimeDiff | 时间戳 | 根据History表查询该用户上一次登录的时间戳，计算当前时刻的时间戳与最近访问时间戳的差值 |
|  | 连接时间 | ContinueTime | 连接持续时间 | 当前会话和观测窗口内历史会话的持续时间  是object类型：  [{  "traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  "connectStart": "2006-01-02 15:04:05.999",  "connectEnd": "2006-01-02 15:04:05.999",  "onlineTime": 82223,  "user\_id": abc,  "termianl\_id":def,  "vm\_id":hj  }] |
|  | 网络地址 | 是否在允许的网段登录 | ifIpAllow | 整型 | 根据在线会话查询接口返回的会话中terminalIp判断网段，查询策略表，判断是否为允许的网段  是-内网：1  是-外网：0  否：-1 |
|  | 是否在允许的地理位置登录 | ifAreaAllow | 整型 | 根据terminnalIp查询地理位置，查询策略表，判断用户是否在允许的地理位置登录，  是-用户单位所在地：1  是-非单位所在地：0  否：-1 |
|  | 安全态势 | 观测时间窗口内触发的告警数量 | terminalAlert | 整型 | 把Suricata的告警存于数据库，查询单位时间窗口内与该terminalIp相关的的安全告警的数量 |

### （2）接入终端（Terminal）节点

采集的特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **特征类型** | **特征名称** | **符号定义** | **数据类型** | **说明** |
|  | 系统 | 终端类型 | terminalType | 整型 | 零终端：1  瘦终端：2  胖终端：3 |
|  | 上次登录用户与本次登录用户是否相同 | userDiff | 整型 | 相同：1  不同：0 |

### （3）虚拟机（VM）节点

采集的特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **特征类型** | **特征名称** | **符号定义** | **数据类型** | **说明** |
|  | 系统 | 系统类型是否符合规则约束 | VMOsAllow | 整型 | 查询到在线会话后，找到ResourceId，根据ResourceId查询虚拟机的信息，找到系统类型，查询策略表，判断虚拟机的操作系统类型是否符合规则的定义  是：1  否：0 |
|  | 系统版本是否符合规则约束 | VMOsVersionAllow | 整型 | 查询到在线会话后，找到ResourceId，根据ResourceId查询虚拟机的信息，找到系统版本，查询策略表，判断虚拟机的操作系统类型是否符合规则的定义  是-高危版本系统：1  是-低危版本系统：0  否：-1 |
|  | 虚拟机性能 | CPU使用率是否超出预置范围 | CPU | 整型 | 查询到在线会话后，找到ResourceId，通过虚拟机性能接口，查询当前 CPU 使用率（0~100%），查询策略表，判断CPU使用率是否符合规则的定义  是且未超过70%：1  是但超过70%：0  否：-1 |
|  | 内存使用率是否超出预置范围 | mem | 整型 | 查询到在线会话后，找到ResourceId，通过虚拟机性能接口，查询当前内存使用率（0~100%），查询策略表，判断内存使用率是否符合规则的定义  是且未超过70%：1  是但超过70%：0  否：-1 |
|  | 连接 | 单位时间内连接的用户数 | VMConnectionUser | 整型 | 查询日志表，获取单位时间窗口内该虚拟机关联的用户数量 |
|  | 登录次数 | VMLoginTotal | 整型 | 查询日志表，获取单位时间内尝试登录该虚拟机的次数 |
|  | 登录成功次数 | VMLoginSucceed | 整型 | 查询日志表，获取单位时间内成功登录该虚拟机的次数 |
|  | 安全态势 | 观测时间窗口内触发的告警数量 | VMAlert | 整型 | 把Suricata的告警存于数据库，查询单位时间内与该虚拟机IP相关的的安全告警的数量 |

# 信任评估流程设计



# 特征预处理

### （1）用户节点

采集特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **特征类型** | **特征名称** | **符号定义** | 权重 | **预处理方法** |
|  | 其他 | 账号类型 | userType | 整型 |  |
|  | 信任值阈值调整因子 | thresholdDelta | 浮点型 | 初始值为0 |
|  | 登录频次 | 尝试登录次数 | loginTotal | w1 | 是可信登录次数阈值，控制在多少次登录后我们才“信得过”这个失败率；  是 Sigmoid 函数，用于将可信度压缩到 [0,1] |
|  | 登录成功次数 | loginSucceed |
|  | 登录时间 | 登录时间段是否存在异常 | ifLoginTimeOK | w2 |  |
|  | 是否偏离习惯登录时间段 | LoginTimeBias |
|  | 最近访问时间距离当前时刻的时间差 | LoginTimeDiff | 0.2 |  |
|  | 网络地址 | 是否在允许的网段登录 | ifIpAllow | w3 |  |
|  | 是否在允许的地理位置登录 | ifAreaAllow |
|  | 其他 | 历史连接信息 | ContinueTime | 连接持续时间 | 当前会话和观测窗口内历史会话的持续时间  是object类型：  [{  "traceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  "connectStart": "2006-01-02 15:04:05.999",  "connectEnd": "2006-01-02 15:04:05.999",  "onlineTime": 82223,  "user\_id": abc,  "termianl\_id":def,  "vm\_id":hj  }] |

### （2）接入终端节点

采集的特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **类型** | **特征名称** | **符号定义** | **权重w2** | **说明** |
|  | 基本信息 | 终端类型 | terminalType | w4 |  |
|  | 上次登录用户与本次登录用户是否相同 | userDiff |
|  | 安全态势 | 观测时间窗口内触发的告警数量 | terminalAlert | w5 |  |

### （3）虚拟机节点

采集的特征包括：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **特征类型** | **特征名称** | **符号定义** | **权重** | **说明** |
|  | 系统 | 系统类型是否符合规则约束 | VMOsAllow | w6 |  |
|  | 系统版本是否符合规则约束 | VMOsVersionAllow |
|  | 虚拟机性能 | CPU使用率是否超出预置范围 | CPU | w7 |  |
|  | 内存使用率是否超出预置范围 | mem |
|  | 连接 | 单位时间内连接的用户数 | VMConnectionUser | w8 | 是可信登录次数阈值，控制在多少次登录后我们才“信得过”这个失败率； |
|  | 登录次数 | VMLoginTotal |
|  | 登录成功次数 | VMLoginSucceed |
|  | 安全态势 | 观测时间窗口内触发的告警数量 | VMAlert | w9 | ) |

# 信任评估算法

## 6.1 节点信任值的计算

出于强可解释性和轻量化的考虑，本文采用了一种简洁的计算方式，首先基于加权求和的方法，分别计算用户节点、接入终端节点、虚拟机节点的信任值，然后建立用户节点-接入终端节点-虚拟机节点的信任转移图，将虚拟机节点、接入终端节点的信任值层层传递至用户节点，最终计算用户的信任得分。

1. 用户节点信任得分

user\_score =

1. 接入终端节点信任得分

terminal\_score = w4 \* + w5 \*

1. 虚拟机节点信任得分

VM\_score = w6 \* + w7 \* + w8 \* connection\_score

+ w9 \*

w1-w9根据重要性决定取值，取值约束如下：

## 6.2 信任传播图的构建

在观测窗口内，用户可能使用多个接入终端，也可能连接多个虚拟机实例，因此观测窗口内的连接关系可以视为图结构。通过6.1章节，我们已经得到了图中不同节点的信任评分，本章节我们将建立远程桌面访问的信任传播图，并建立虚拟机->接入终端->用户之间信任逐层传递的机制。

### 6.2.1 符号定义

假设观测窗口内，用户x使用了N个接入终端，其中，第个接入终端在观测窗口内访问了M个虚拟机实例。用户x使用接入终端对M个虚拟机实例的连接持续时间分别为，用户x使用接入终端的连接时间

### 6.2.2虚拟机到接入终端信任值的汇聚

“连接”代表用户对虚拟机的访问链路。接入终端的信任值是由虚拟机节点的信任值汇聚得到的。接入终端的信任值表示为：

其中，由连接持续时间决定，

### 6.2.3 接入终端到用户信任值的汇聚

与6.2.2章节的汇聚方法类似，用户信任值由用户节点信任得分、观测时间窗口内接入终端的信任值汇聚得分、时间衰减因子求和得到。

+0.2\*

其中，

# 7 动态访问控制策略的生成

## 7.1 访问控制策略

（1）二次身份认证

（2）限制访问

（3）封禁用户

（4）允许访问

## 7.2 动态访问控制策略的生成

1. 规则触发：根据规则定义的访问控制策略执行
2. 信任评分低于阈值触发，初始阈值设置如下：
3. ：允许访问
4. ：二次身份认证
5. ：限制访问
6. ：封禁用户
7. 规则的推送：信任评分低于阈值而触发的访问控制策略应推动给管理员，由管理员决定是否进行处置

## 7.3 信任阈值的调整

当用户完成二次身份认证、或通过线下方式证明其身份合法性后，应自动调整信任阈值调整因子:

thresholdDelta = thresholdDelta+